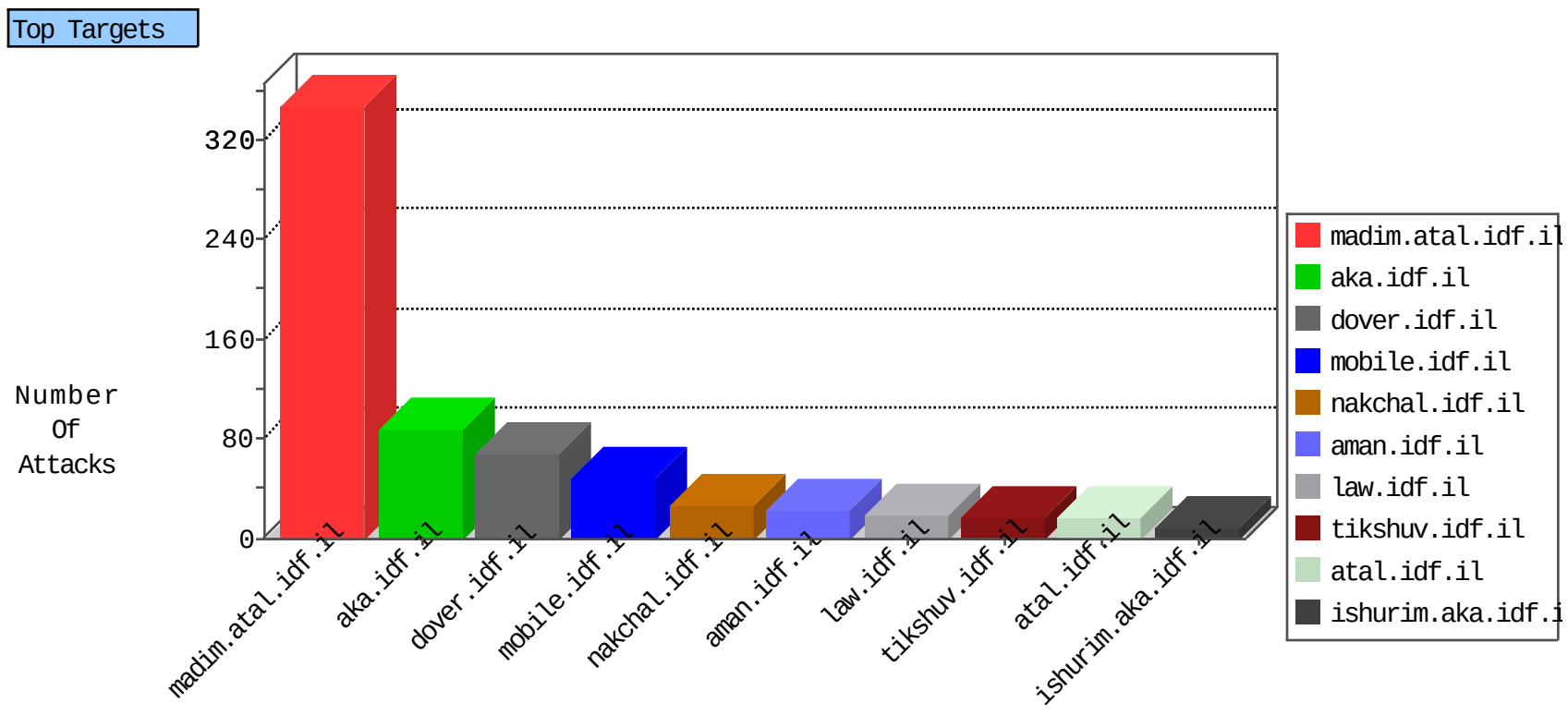
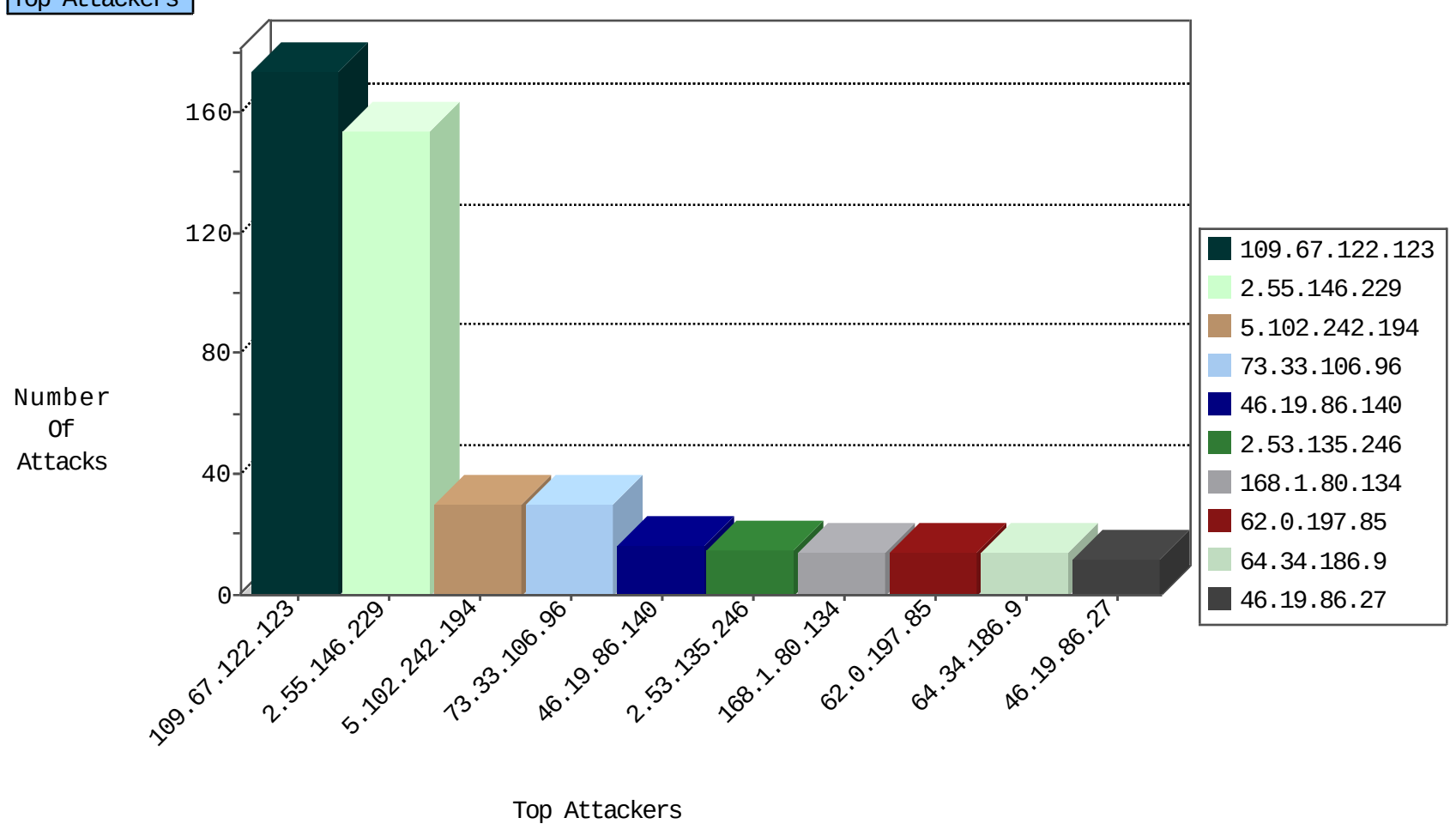
09-23-2016-09:04:00 to 09-23-2016-10:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-09:04:00 to 09-23-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.146.229	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
79.180.206.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
173.244.198.5	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

09-23-2016-09:04:00 to 09-23-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.34.186.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-23-2016-09:04:00 to 09-23-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
168.1.80.134	147.237.77.233	Australia	atal.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
198.199.89.155	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
198.199.89.155	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.8.50	Pakistan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.83.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
211.149.246.60	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.124.232.86	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.161.40.17	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.232.86	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
198.199.89.155	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.10	147.237.77.74	Ukraine	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.232.110.28	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.73	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
211.149.197.148	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.232.86	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1

09-23-2016-09:04:00 to 09-23-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
109.67.122.123	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
109.67.122.123	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	12
84.108.30.21	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
73.33.106.96	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
73.33.106.96	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
73.33.106.96	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.86.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.66	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.138.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.135.246	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.140	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.246.136.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
118.172.21.145	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.101.148.34	Germany	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
45.56.101.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.132.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.36	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.53.135.246	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.53.135.246	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.135.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.138.60	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
89.237.68.166	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.132.107.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.117.150.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.116.214.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.186.113.132	Japan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
83.130.79.158	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
176.13.227.1	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.127.36.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.161.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.236.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.94.76.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.66	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.32.179.167	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.22.134.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.63	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.138.83	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.199.89.155	United States	147.237.0.35	akaws.idf.il	drop		drop	1

09-23-2016-09:04:00 to 09-23-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.122.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
2.55.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.40.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.81.2	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.79.141	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/7/697.doc	Block	1
46.19.85.170	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
104.237.151.219	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
31.154.81.2	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
157.55.39.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kiosk	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
67.82.249.71	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/login/	Block	1
46.19.85.170	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method .il/901-8544-he/tikshuv.aspx in URL	Block	1
109.67.55.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3416.jpg	Block	1
37.142.125.227	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.73	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
84.109.129.208	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.228.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.75.149	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
40.77.167.93	Reunion	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
180.76.15.28	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.64.210.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
80.246.136.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.194.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.79.137	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
46.19.85.170	Israel	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
104.236.53.155	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
80.246.140.203	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-23-2016-09:04:00 to 09-23-2016-10:04:00